AO 91 (Rev. 11/11) Criminal Complaint (approved by AUSA Sarah Wolfe)

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America
v.
Reginald Adams, a/k/a "Reggie Adams"

Case No. 22-mj-1264

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2020 to August 2021 in the county of Philadelphia in the Eastern District of Pennsylvania, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1343 (wire fraud)	Knowingly and intentionally did devise and intend to devise a scheme and artifice to defraud young women of their property by means of false or fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, did knowingly and intentionally transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely a text message on or about August 5, 2021 to VICTIM 1 in Philadelphia, Pennsylvania, from a place outside of Pennsylvania.

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

s/ Andrew Davis
Complainant's signature

Andrew Davis, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 08/09/2022 at 2:32 pm

s/ Hon. Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

The Hon. Richard A. Lloret, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Andrew Davis, being first duly sworn, hereby depose and state as follows:

A. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a Criminal Complaint and Arrest Warrant against REGINALD ADAMS a/k/a "REGGIE ADAMS." As set forth below, there is probable cause to believe that, from in or around May 2020 to in or around August 2021, ADAMS knowingly and intentionally did devise and intend to devise a scheme and artifice to defraud young women of their property by means of false or fraudulent pretenses, representations, and promises, that is, ADAMS sent messages to individuals throughout the United States, falsely representing that he was an employee of Provider A, amongst other false representations, in an effort to obtain online account access, data, sexually explicit photographs, and other personally identifiable information, when in fact, ADAMS was not employed by Provider A. Moreover, there is probable cause to believe that, on August 5, 2021, for the purpose of executing such scheme and artifice, ADAMS did knowingly and intentionally transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely, a text message to VICTIM 1 in Philadelphia, Pennsylvania from a place outside of Pennsylvania, in violation of Title 18, United States Code, Section 1343.

2. I have been employed as a Special Agent with the FBI since May 2017 and am currently assigned to the Philadelphia Division's Cyber Crime Squad, whose primary mission is to investigate crimes involving computers and the Internet. While employed with the FBI, I have investigated and participated in investigations involving federal criminal violations related to computers and the Internet, along with other federal violations. I have attended training at the

FBI Academy, training involving computers and networking technology, including becoming certified as a Computer Analysis Response Team (CART) Technician, and training on various topics in cyber crime. Prior to being employed with the FBI, I was a cyber threat analyst in the private sector for four years, studying targeted network attacks against Defense Industrial Base (DIB) companies. Prior to that, I worked as a systems administrator in the private sector for six years. Based upon my training and experience, I am familiar with the means by which individuals use computer and information networks such as the Internet to commit various criminal offenses, and I have participated in the execution of searches and seizures pursuant to warrants authorizing the seizure of evidence related to computer crimes.

3. This affidavit is based on my personal knowledge and information obtained from documents, witnesses, and other law enforcement officials. The information contained in this affidavit is submitted for the limited purpose of establishing probable cause in support of a criminal complaint and arrest warrant against REGINALD ADAMS. As such, this affidavit does not include all of the information that I have acquired while participating in this investigation. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date asserted. Similarly, where I assert that an event took place a certain number of times, I am asserting that the event took place approximately the number of times asserted.

B. STATEMENT OF PROBABLE CAUSE

4. At all times relevant to this Complaint:

a. Provider A was an electronic messaging application that provided users the ability to engage in private conversations, with chat and/or video, and to publish content viewable by other users;

b. Provider B was a text messaging application that provided users the ability to send text messages using different phone numbers; and

c. Website 1 was a popular social news website.

5. On August 12, 2021, the FBI was advised that a 23 year-old female ("VICTIM 1") residing in Philadelphia, PA had been victimized by an unknown subject who had hacked into her account on Provider A, obtained a partially nude photo of her, and sent the photo to multiple male contacts from her account. The subject had also posted the partially nude photo and personally identifying information for VICTIM 1 to Website 1. As a result, VICTIM 1 began receiving frequent friend requests via Provider A and text messages from individuals who had seen her photo and wanted additional photos of VICTIM 1.

Victim Interviews and Analysis of Records

6. On August 16, 2021, FBI interviewed VICTIM 1, who provided the following information:

a. VICTIM 1 reported that, on August 5, 2021, she received text messages from telephone number 301-679-5716. The text messages appeared to be sent from Provider A's official staff to alert VICTIM 1 to unusual login activity on VICTIM 1's account. In these texts, the subject, later identified by law enforcement as REGINALD ADAMS ("ADAMS"), requested that VICTIM 1 provide a security code that had been sent to VICTIM 1's device to avoid having the account locked. (Unbeknownst to VICTIM 1, ADAMS had previously sent a request to Provider

A to reset the password of VICTIM 1's account. In response to the password reset request, Provider A sent a security code to VICTIM 1's phone.) Accordingly, VICTIM 1 provided the code to ADAMS.

b. The following day, VICTIM 1 tried to open her Provider A account, but discovered that she had been logged out. Later that day, VICTIM 1 received text messages from friends about a photo sent from VICTIM 1's Provider A account. VICTIM 1 was unable to log back into her account and had to reset the password. After re-establishing access, VICTIM 1 learned that a partially nude photo of her that had been in her Provider A private photo collection had been sent via Provider A to approximately 50 male friends from VICTIM 1's contact list. One of these friends, J.H., told VICTIM 1 about another person ("VICTIM 2") in their hometown who had experienced a similar attack.

c. VICTIM 1 contacted VICTIM 2, who confirmed that she was also a victim of a Provider A account compromise and had private photos of her posted on Website 1. With the assistance of VICTIM 2, VICTIM 1 found her own photos and personal information posted on Website 1.

7. On August 19, 2021, J.H. was interviewed by the FBI and confirmed that he had received the partially nude photo of VICTIM 1 from VICTIM 1's Provider A account on August 6, 2021. J.H. explained that, shortly thereafter, someone named "Trey White" with username "twhizzle18" added J.H. as a friend on Provider A. The twhizzle18 account user sent J.H. two messages. The first message included approximately eight photos, some nude, of women J.H. recognized as friends from his high school in Chambersburg, Pennsylvania. In the second

message, twhizzle18 asked if J.H. wanted to see more. J.H. did not respond and instead blocked the twhizzle18 account and reported it to Provider A.

8. According to subscriber records from Provider B, the phone number (301-679-5716) that had sent VICTIM 1 the above-described fraudulent text messages seeking the code for her Provider A account was registered to "reggie.adams34" at that time. The records further revealed that the account was registered with email address reggie.adams34[@]gmail.com.

9. On August 27, 2021, a federal search warrant authorized by the Honorable Richard A. Lloret, United States Magistrate Judge in the Eastern District of Pennsylvania was executed for the Provider B account reggie.adams34. The Provider B records revealed the content of text messages to and from the reggie.adams34 account as well as a list of other phone numbers that had been assigned to the account. In reviewing the records, I observed that the account was used repeatedly to compromise numerous Provider A accounts and buy photos from women. Specifically, from December 2020 through August 2021, the account was assigned 12 different phone numbers, all of which were used to send text messages to women in an effort to compromise their Provider A accounts. Among the texts was a message sent to VICTIM 1's phone number on August 6, 2021 at 1:15 a.m. UTC (or August 5, 2021 at 9:15 p.m. EDT) that stated:

> Uh oh! [Provider A] has detected unusual activity on your account, [VICTIM 1]. A login attempt was made from "Josh's iPhone 12" near Shippensburg, Pennsylvania 10:28:17 EDT 6 August 2021. In order to secure your account, please reply with the 6 digit security code sent to your device. Do not share or use elsewhere!

These records are consistent with the information VICTIM 1 reported to the FBI during her interview, as discussed above. According to VICTIM 1, she was located in Philadelphia, Pennsylvania on August 5, 2021, when she received the above text message.

10. On September 3, 2021, FBI interviewed VICTIM 2, who stated that she was also a victim of this same scheme starting in July 2020 and continuing through February 2021. VICTIM 2 showed interviewing agents one of the text messages she received, purportedly from Provider A's official staff, requesting the password for her account on Provider A. The text message was sent on February 22, 2021 from 213-263-7585. According to records from Provider B, that phone number (213-263-7585) was assigned to reggie.adams34 on that date.

11. According to subscriber records from Provider A, the registered phone number for the twhizzle18 account at the time of account creation was the same phone number (213-263-7585) that texted the fraudulent message to VICTIM 2 on February 22, 2021. VICTIM 1 and VICTIM 2 each advised that the twhizzle18 account had attempted to add both of them as friends on the Provider A platform shortly after their accounts had been compromised. Neither VICTIM 1 nor VICTIM 2 accepted the twhizzle18 account as a friend.

12. Furthermore, records from Google revealed that the reggie.adams34[@]gmail.com account received emails from Provider A, Provider B, and Website 1. As described above, all of these services were utilized in furtherance of this criminal scheme.

13. On August 23, 2021, FBI interviewed VICTIM 3. According to VICTIM 3, on May 16, 2020, she began receiving text messages, purportedly from Provider A, indicating that there was a suspicious login attempt for her account and requesting that she confirm a security code that Provider A had sent to her device. VICTIM 3 advised that she talked to ADAMS, who she knew from high school, about these text messages and ADAMS encouraged her to cooperate with the sender to protect her account. VICTIM 3 followed ADAMS' advice and provided the code to the sender of the text message, but was subsequently locked out of her Provider A

account. When VICTIM 3 relayed this to ADAMS, he offered to hack into her account and claimed he could break Provider A's two-factor authentication, but would need her old passwords to do so. VICTIM 3 did not provide any of her old passwords to ADAMS. VICTIM 3 also advised that she has been unable to regain access to her compromised Provider A account. Further, VICTIM 3 advised that, in November 2020, she received a text message from an unfamiliar phone number. According to VICTIM 3, the sender asked to buy photos from VICTIM 3 and directed her to send the photos to Provider A account "bshmurda9."[1]

14. VICTIMS 1-3 all advised that they knew ADAMS, as they all went to the same high school in Chambersburg, Pennsylvania. Additionally, the victims all stated that they were friends with ADAMS on Provider A's platform.

15. VICTIMS 1-3 also identified other social media accounts that ADAMS used, including two additional accounts on Provider A's platform ("theregetable" and "reggieadams2") and one on Twitter ("theREGetable"). Records from Provider A and Twitter revealed that all three accounts were associated with phone number 717-830-6937.

16. According to records provided by AT&T, phone number 717-830-6937 was associated with an Apple iPhone XR with IMEI[2] (International Mobile Equipment Identity) number 357342094383622.

---

1 The bshmurda9 account was subsequently attributed to ADAMS through overlapping IP addresses and ADAMS' confession, as discussed further below.

2 According to Verizon, the IMEI, or International Mobile Equipment Identity, is analogous to a fingerprint for a phone. The IMEI is a 15 digit number that is unique to each device and standardized across the industry. *See* https://www.verizon.com/articles/what-to-know-when-buying-a-used-phone/ (last accessed October 1, 2021).

17. Records from Apple revealed that an Apple iPhone XR with the above-referenced IMEI was registered to REGGIE ADAMS, with phone number 717-830-6937 and Apple ID reggieadams99[@]yahoo.com.

18. During the review of the records provided by Providers A, B, Yahoo, Twitter and Apple, some IP addresses (Internet Protocol Addresses) were consistent across accounts. That is, each of these accounts was accessed from the same IP addresses during this time period, often multiple times. For example, from August 14, 2021 to August 20, 2021, IP address 107.77.201.124 accessed multiple accounts a total of 98 times, and at times accessed multiple accounts within seconds of each other.

19. Another IP address that was frequently observed in account login records was 67.161.149.221, as revealed in records obtained from Providers A, B, Google, Twitter, Apple, and Mega.nz. The following table provides a summary of the usage of this IP address based on these records:

Provider	Username	Date Range	Access Count
Twitter	theregetable	6/21/2021 - 7/3/2021	8
A	twhizzle18	3/30/2021 - 8/9/2021	1274
A	bshmurda9	3/30/2021 - 10/5/2021	1237
B	reggie.adams34	8/6/2021 - 8/9/2021	17
Google	reggie.adams34[@]gmail.com	8/4/2021 - 8/29/2021	278
Apple	reggieadams99[@]yahoo.com	9/20/2021 - 10/7/2021	4208
Mega.nz	reggie.adams34	4/2/2021 - 10/5/2021	3

20. According to subscriber records from Comcast, on the relevant dates, IP address 67.161.149.221 was assigned to a residence located at 1817 W Horsetooth Rd, Fort Collins, Colorado 80526-2322.

21. Pursuant to a federal search warrant issued on October 7, 2021 by the Honorable Lynne A. Sitarski, United States Magistrate Judge in the Eastern District of Pennsylvania, Apple

produced account records for the Apple ID reggieadams99[@]yahoo.com, which included records stored in ADAMS' iCloud account. During the review of these records, I observed a screenshot of a March 22, 2021 email conversation between REGGIE ADAMS and a prospective landlord for "1817 Horsetooth" confirming that a rental application from ADAMS and two other individuals had been approved. I also observed a photo stored in the account showing the last page of a lease signed on March 25, 2021. Three printed names and signatures were on the lease, including REGINALD ADAMS.

22. On November 10, 2021, United States Magistrate Judge S. Kato Crews of the District of Colorado issued a search warrant authorizing the tracking of precise location information and data/GPS information on the cellular telephone assigned call number 717-830-6937. Information obtained pursuant to this warrant informed investigators that ADAMS was living at his residence in Fort Collins, Colorado and driving regularly to Wyoming. According to records obtained from the United States Air Force, ADAMS enlisted in the Air Force on December 19, 2017 and was assigned to the 90th Medical Group at the FE Warren Air Force Base in Cheyenne, Wyoming.

Search and Interview of REGINALD ADAMS

23. On November 23, 2021, FBI and Air Force Office of Special Investigations (OSI) Special Agents executed a search of ADAMS' person, pursuant to a search warrant issued on November 22, 2021 by the Honorable Kelly H. Rankin, Chief United States Magistrate Judge in the District of Wyoming. Agents recovered an iPhone XR, assigned phone number 717-830-6937 and IMEI 357342094383622, from ADAMS' pocket.

24. That same day, after being advised of his rights via an FBI Advice of Rights form, ADAMS agreed to be interviewed by FBI. During the interview, ADAMS admitted that he

began hacking Provider A accounts in approximately 2020, and that he learned how to do it from various posts on Website 1.

25. Specifically, ADAMS stated that a Website 1 user provided ADAMS with a script that he used to trick girls into providing the security code for their Provider A accounts. The script started with, "Uh Oh! [Provider A] has detected an unusual activity on your account" and ended with, "in order to secure your account, please reply with a 6-digit code sent to your device." This is the text message that several victims in this case reported receiving.

26. ADAMS said he used the Provider B application to obtain different phone numbers, and he texted the females pretending to be Provider A official staff. Once ADAMS obtained the security code, he logged into the victim's account, looked through photos, downloaded the photos he wanted, and posted some to Website 1.

27. ADAMS stated that he also operated several other Provider A accounts. These monikers included twhizzle18, bshmurda9, djoe543, djoe419, bigwilley819, sugarman461, and papasmurf8. During this interview, ADAMS admitted that he was responsible for hacking VICTIM 1's account, as well as at least 20 other victims. Moreover, ADAMS admitted that he created an impersonation account for VICTIM 11.

28. After extracting the contents of ADAMS' iPhone XR, agents returned the device to ADAMS and instructed him to discontinue all contact with victims during the ongoing criminal investigation. Subsequent review of the contents of ADAMS' iPhone XR revealed several installed applications, including Mega.ios, VPN software, Kik, and Website 1, all of which were used by ADAMS as part of this hacking scheme.

ADAMS' Post-Interview Conduct

29. Following the search and interview of ADAMS, multiple victims began reporting new activity from the same Provider A accounts that ADAMS had told the FBI he controlled. For example:

a. On February 16, 2022, two victims, VICTIM 10 and VICTIM 4, reported receiving friend requests from a Provider A account resembling the name of VICTIM 11. This Provider A account is the same impersonation account for VICTIM 11 that ADAMS previously admitted to creating.

b. On March 8, 2022, VICTIM 4 reported that she had been added by accounts sugarman461 and djoe543, which ADAMS previously admitted to using.

c. On March 9, 2022, VICTIM 5 reported that she was recently added by the account bshmurda9, which ADAMS previously admitted to using.

d. On March 10, 2022, VICTIM 2 reported that VICTIM 6 received a friend request from bigwilley819, and VICTIM 7 received requests from a djoe account, as well as sugarman, bigwilley, and reggieadams. VICTIM 2 also advised that she had received an image of an unknown male's exposed genitals.

30. Other victims reported that they received text messages containing explicit photos from unfamiliar telephone numbers. For example:

a. On February 19, 2022, VICTIM 8 reported that she received an unsolicited text message from 510-806-9648 containing an image of an unknown male's exposed genitals. Agents have identified this telephone number as being associated with Provider B.

b. On March 5, 2022, VICTIM 9 reported that she received an unsolicited text message from 312-622-9915 containing a partially nude photograph of an unknown female.

c. On March 8, 2022, VICTIM 3 reported that she received an unsolicited text message from 510-806-9648 that read, "Still don't believe me? Or is it time to hold up your end of the bet." The user sent the same image that was sent to VICTIM 8, depicting an unknown male's exposed genitals.

31. According to records from Provider B, the phone number (510-806-9648) that texted VICTIM 3 on March 8, 2022 was assigned to user greenbeans6411 with registration IP address 47.45.155.128, registered on February 17, 2022. This same IP address was used to access the reggie.adams34@gmail.com account on August 26, 2021 and August 29, 2021, and to access ADAMS' iCloud account between August 26, 2021 and September 2, 2021.

32. In addition, in reviewing the Apple records for ADAMS' iCloud account (obtained pursuant to the October 7, 2021 search warrant, as discussed above in paragraph 21), agents observed images of male genitalia that were consistent with the photos described above.

C. CONCLUSION

33. Based on the above, I believe probable cause exists that, from in or around May 2020 to in or around August 2021, in the Eastern District of Pennsylvania, REGINALD ADAMS a/k/a "REGGIE ADAMS" committed a violation of Title 18, United States Code, Section 1343 (wire fraud).

s/ Andrew Davis
Andrew Davis, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me on August 9, 2022

s/ Honorable Richard A. Lloret
THE HONORABLE RICHARD A. LLORET
United States Magistrate Judge
Eastern District of Pennsylvania